

AFFIDAVIT OF JASON J. DEFREITAS IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jason J. DeFreitas, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security (DHS) United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) assigned to the Boston Field Office and have been employed by HSI since 2006. I am currently assigned to the Cyber Group. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with ICE HSI, I served as a United States Customs and Border Protection (CBP) officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States laws.
2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the residence located at 56 Saint Joseph St., Apt. 510, Fall River, Massachusetts 02723 (the "SUBJECT PREMISES"), the vehicle registered to Michael PAIVA, a red Toyota Camry with Massachusetts registration 5MY459 (the

“SUBJECT VEHICLE”), and the person of Michael PAIVA (YOB 1982), as more fully described in Attachment A, which is incorporated herein by reference.

3. As described herein, there is probable cause to believe that the SUBJECT PREMISES, SUBJECT VEHICLE, and the person of PAIVA contain contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, which items are more specifically described in Attachment B, which is also incorporated herein by reference.
4. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (possession, receipt, and distribution of child pornography) are presently located at the SUBJECT PREMISES, within the SUBJECT VEHICLE, and on the person of PAIVA.

BACKGROUND ON KIK AND KIK REPORTS

5. Kik Messenger (hereinafter “Kik”) is a mobile application designed for chatting or messaging owned and operated by Kik Interactive, Inc. According to the publicly available document “Kik’s Guide for Law Enforcement,”¹ to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the

¹ Available at: <https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement>.

application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

6. According to “Kik’s Guide for Law Enforcement,” Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.
7. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik’s Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen, and delete user content at any time if Kik believes use of their services is in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

8. Kik is located in Ontario, Canada and is governed by Canadian law. According to information contained in the “Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary” (hereinafter Kik Glossary), which Kik provides when reporting information to law enforcement authorities, Kik is mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law that are discovered on the Kik platform. According to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third party moderators.
9. The RCMP has advised Homeland Security Investigations (HSI) agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviews the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provides Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provides the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

STATEMENT OF PROBABLE CAUSE

10. I have reviewed a Kik Report dated November 20, 2018. A review of the Kik Report shows that between July 29, 2013 and November 20, 2018 a Kik user, “harveydangermouse_p63” who provided the name “Mr. Mike”, email address michaelpaiva@comcast.net, and a Verizon SM-N920V phone used Kik to send an image of child pornography, as described herein.

11. I have learned that Kik was alerted to the child pornography through use of Microsoft's PhotoDNA technology. According to the Kik Glossary, Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a Report and sends it to the Kik Law Enforcement team. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via a PhotoDNA Report, as well as any related user communications, are visually reviewed by a member of the Kik Law Enforcement Response team before a report is forwarded to law enforcement authorities. Kik trains employees comprising its Law Enforcement Response team on the legal obligation to report apparent child pornography. The Team is trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovered the suspected child pornography, Kik removed the content from its communications system and closed the user's account.
12. Along with Kik's Report, Kik provided copies of the suspected child pornography image that they located to the RCMP. On May 6, 2019, I reviewed the very same image that Kik had provided with the Kik Report sent to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched, and viewed by Kik personnel before they were reported to the RCMP. I reviewed only the image previously located, isolated, searched,

and viewed by Kik personnel and observed that the image is child pornography as defined by Federal Law

13. Specifically, the image distributed by Kik user “harveydangermouse_p63” depicts a naked, prepubescent female child between the ages of 1-2 years-old lying on her back with her legs spread open exposing the child’s vagina. An adult, erect penis can be seen resting on the child’s vagina.
14. The information provided by Kik included IP addresses² associated with access to the subject Kik user account. Specifically, IP address 174.192.30.42 was used by harveydangermouse_p63 on November 20, 2018 at 13:48:22 (UTC) to send the above described child pornography image. In addition, IP address 73.100.83.52 was used to access the subject Kik user account during the same month that the described image of child pornography was sent.
15. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that IP address 174.192.30.42, used to send the described image of child pornography, was

² An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

registered to Verizon Wireless. The other IP address, 73.100.83.52, was registered to Comcast Cable Communications, LLC (“Comcast”).

16. On or about January 28, 2019, an administrative summons was issued to Verizon Wireless for information relating to the IP address used to send the described image of child pornography. A review of the results obtained on or about March 1, 2019, identified that the IP address was used in association with telephone number (508) 930-7314, with subscriber information as follows:

Account Number: 585883956-1
Name: Jacqueline Pinto
Address: 87 Mellen St., Brockton, MA 23011

17. On or about January 28, 2019, an administrative summons was issued to Comcast for information relating to the other IP address, 73.100.83.52, used by “harveydangermouse_p63” during the same month that the described image of child pornography was sent. A review of the results, obtained on or about January 29, 2019, identified the following account holder and address:

Subscriber Name: Denice Hatch
Service Address: 34 Nicholson Drive, Brockton, MA
Account Number: 8773101901963391
Account Status: Active
Type of Service: High Speed Internet Service

18. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Michael J. PAIVA. These public records indicated that PAIVA’s current address is 56 Saint Joseph St., Apt. 510, Fall River, MA 02723 (the “SUBJECT PREMISES”).

19. A check with the Registry of Motor Vehicles (“RMV”) on or about May 8, 2019, revealed that Michael PAIVA with a year of birth of 1982 is assigned a Massachusetts driver’s license and is listed as the lessee on the registration for a Toyota Camry assigned Massachusetts registration number 5MY459, the SUBJECT VEHICLE. Both PAIVA’s driver’s license and the registration for the SUBJECT VEHICLE list PAIVA’s current address as 56 Saint Joseph St., Fall River, MA. According to RMV records, PAIVA listed 87 Mellen Street, Brockton, MA as a previous mailing address (this is the address associated with the subscriber information for the Verizon Wireless account used to send the described image of child pornography (see Paragraph 16)).
20. On or about April 19, 2019, members of the Fall River Police Department (FPD) conducted a ruse at the SUBJECT PREMISES. Although FPD did not make contact with anyone at the SUBJECT PREMISES, they spoke with a neighbor who confirmed that someone with the name of Michael PAIVA, who is employed as an Uber driver, resides at the SUBJECT PREMISES. The mail box for the SUBJECT PREMISES listed the names of Michael PAIVA and Katherine Hatch.
21. From open source information and a review of the Brockton Public Schools District’s (“BPSD”) fiscal year (“FY”) 2018 budget, it was revealed that a person with the name of Michael PAIVA was employed at an elementary school with the BPSD as a paraprofessional. Also, the BPSD’s FY 18 budget listed a person with the name of Katherine Hatch as an employee at the same elementary school. Furthermore, a review of the BPSD’s FY 2019 budget listed persons with the name of: Denice Hatch employed as a secretary; and Jacqueline Pinto employed as a computer tech. According to information

received from a member of the Brockton Police Department, who oversees the Brockton Police's School Resource Program, PAIVA is no longer employed with BPSD and Jacqueline Pinto, the subscriber for the Verizon wireless account described in paragraph 16, is PAIVA's mother and is still employed with the school district.

22. From a review of Katherine Hatch's Facebook page, I observed numerous photographs posted to that account that appeared to depict both Katherine Hatch and PAIVA together. Katherine Hatch's Facebook account listed another account in the name of "Michael Joseph" as a friend. Based on content, including numerous photographs of PAIVA and information that lists "Michael Joseph's" employment as an Uber and Lyft driver, I conclude that this is PAIVA's Facebook account.
23. Katherine Hatch's Facebook account also listed another account in the name of Denice MacNeill Hatch, the same name of the subscriber of the Comcast account described in paragraph 18, as a friend. I reviewed Denice MacNeill Hatch's Facebook account and observed a photograph of her with PAIVA and Katherine Hatch.
24. On or about May 6, 2019, an administrative summons was issued to Uber Technologies in regard to information relating to drivers with PAIVA's name and his Massachusetts driver's license number. A review of the results received on or about May 8, 2019, confirmed that PAIVA is driver for UBER and listed the following pertinent information:

Name: Michael PAIVA
Phone Number: 508-930-7314³

³ This is the same telephone number listed on the Verizon Wireless account described in paragraph 16.

Email Address: Michaelpaiva@comcast.net⁴

Vehicle Information: 2017 Toyota Camry 5MY459 ⁵

Address per Profile: 56 St. Joseph St., Apt. 510, Fall River, MA 02723 ⁶

25. During surveillance of the SUBJECT PREMISES on or about May 2, 2019, I observed a vehicle registered to Katherine Hatch parked in a parking lot belonging to the apartment complex where the SUBJECT PREMISES is located.⁷ On or about May 9, 2019, at approximately 7:21 AM, a FPD Detective observed the SUBJECT VEHICLE parked in a parking lot belonging to the same apartment complex where the SUBJECT PREMISES is located.
26. On or about May 8, 2019, I used an iPhone wireless device in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES and at 34 Nicholson Dr., Brockton, MA (the "BROCKTON ADDRESS"). While positioned directly across from both the SUBJECT PREMISES and the BROCKTON ADDRESS, I noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that network. Based on the signal strength of the wireless networks, the names, or Service Set Identifiers, of the wireless networks, as

⁴ This is the same email address that was listed on the harveydangerouse_p63 Kik account describer in paragraph 10.

⁵ The SUBJECT VEHICLE.

⁶ The SUBJECT PREMISES.

⁷ RMV records indicated that a 2010 Chevy Cobalt, registration #: 58GW84, is registered to Katherine Hatch at the SUBJECT PREMISES. Katherine Hatch's Massachusetts Driver's License listed her residential address as 56 Saint Joseph St., Fall River, Massachusetts 02723.

well as my training and experience and information relayed to me by agents, I believe that the wireless router at the SUBJECT PREMISES and the BROCKTON ADDRESS is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

27. I have had both training and experience in the investigation of computer-related crimes.

Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable, or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.
- c. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally

millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer, smartphone, or other internet-capable device.

- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - including computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones are also often carried on an individual's person.
- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet.

Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

- g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored
- h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

28. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, advertise, transport, distribute, receive, possess, and/or access with intent to view child pornography (i.e., “consumers” of child pornography):
- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
 - b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including in “hard copy” and electronic format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
 - c. Such individuals almost always possess and maintain their hard copies of child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children and who have hard copies of child pornographic material typically retain that material for many years.
 - d. Likewise, such individuals often maintain their digital or electronic child

pornography in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

- e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.⁸
- f. Such individuals also may correspond with and/or meet others to share information and materials, often retain correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information for individuals with whom they have been in contact and who share the same interests in child pornography.

⁸ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

- g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
 - h. Even if PAIVA uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES as well as in his vehicle or on his person, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).
29. Based on the facts described herein, there is probable cause to believe that Michael J. PAIVA is an individual who distributed and possesses child pornography on computer equipment capable of accessing the internet. Based on all the foregoing, there is probable cause to believe that PAIVA lives at the SUBJECT PREMISES and drives the SUBJECT VEHICLE. Given that consumers of child pornography usually keep their child pornography and related materials in a safe and private location, I submit that there is probable cause to believe that evidence of the SUBJECT offense will be found at the SUBJECT PREMISES, within the SUBJECT VEHICLE, and on the person of PAIVA.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, within the SUBJECT VEHICLE, and on the person of PAIVA, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer’s hard drive or other

storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, within the SUBJECT VEHICLE, or on the person of PAIVA, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

- a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
32. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES, within the SUBJECT VEHICLE, or on the person of PAIVA, because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and

the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for

evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:
 - a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;
 - b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover

“hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

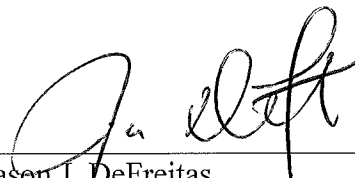
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or

encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

35. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.




Jason J. DeFreitas
Special Agent
Homeland Security Investigations

Sworn and subscribed to before me this ¹⁴ day of June, 2019.

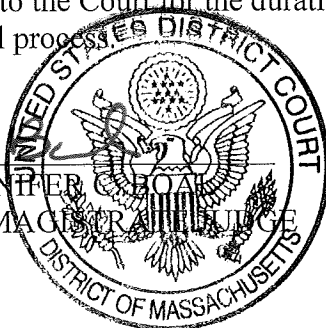


HONORABLE JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE

I have reviewed the image referenced in paragraph 13 above, and I find probable cause to believe that the image depicts a minor engaging in sexually explicit conduct. The Affiant shall preserve the image provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.



HONORABLE JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

LOCATION TO BE SEARCHED

The property located at 56 Saint Joseph St., Apt. 510, Fall River, Massachusetts 02723 (the SUBJECT PREMISES), which is described as an apartment located with The Falls apartment complex located on the north side of Saint Joseph Street. The SUBJECT PREMISES is located on the fifth floor of the building. The entrance to the SUBJECT PREMISES is a green-in-color door with “510” in white numbering located in its center. The SUBJECT PREMISES is pictured below:



ATTACHMENT A

LOCATION TO BE SEARCHED

The SUBJECT VEHICLE is a red Toyota Camry, assigned Massachusetts Registration #: 5MY459.

ATTACHMENT A

PERSON TO BE SEARCHED

Michael J. PAIVA, YOB 1982, is pictured below:



ATTACHMENT B

ITEMS TO BE SEIZED

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2252A, including:
 - A. Records and tangible objects pertaining to the following topics:
 1. Child pornography and child erotica; and
 2. Communications with any other person that relates to the sexual exploitation of children.
 - B. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant, belonging to or used by MICHAEL J. PAIVA (“the computer equipment”):
 1. evidence of who used, owned, or controlled the computer equipment;
 2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;
 3. evidence of the attachment of other computer hardware or storage media;
 4. evidence of counter forensic programs and associated data that are designed to eliminate data;
 5. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events

- relating to the crime(s) under investigation and to the computer user;
 - 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
 - 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and
 - 8. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - 9. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
 - 10. documentation and manuals that may be necessary to access the computer equipment or to conduct a forensic examination of the computer equipment;
 - 11. records of or information about Internet Protocol addresses used by the computer equipment;
 - 12. records of or information about the computer equipment's Internet activity; and
 - 13. contextual information necessary to understand the evidence described in this attachment.
- C. Records, information, and items relating to the ownership or use of computer equipment and other electronic storage devices found in or on the LOCATION TO BE SEARCHED.

- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If the computer equipment contains contraband, it will not be returned. If the computer equipment cannot be returned, agents will attempt to make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband or the fruits or instrumentalities of crime.